2003年5月　　安徽教育学院学报　　May. 2003
第21卷第3期　　Journal of Anhui Institute of Education　　Vol 21 No. 3

一类形式素数的无穷性

潘杨友
(池州师范专科学校 数学系, 安徽 池州 247000)

[摘　要] 本文运用了欧几里德证明素数无穷性方法及数学分类思想, 结合二次剩余、数关于模m 的阶和费马数的特征, 系统地证明了形如: $4n+k(n\in N, k=\pm1)$, $8n+k(n\in N, k=1、3、5、7)$形式素数的无穷性。并结合群论与数论研究的相辅关系, 利用有限群特征标理论与性质证明了狄利克雷定理。

[关键词] 费马数, 数模m 的阶, 二次剩余, 勒让德符号, 特征标。
[中图分类号] O184　　[文献标识码] A　　[文章编号] 1001-5116(2003)03-0008-03

1　形如$4n+k(n\in N, , k=\pm1)$形式素数的无穷性

命题1　形如$4n-14n+k(n\in N)$的素数有无穷多个。

[分析]欧几里德(Euclid)在证明素数无穷性时所运用的是构造法, 其思想是先反设素数仅有有限个, 然后利用它们构造出一个新的异于它们的素数P。现反设形如$4n-1(n\in N)$的素数仅有有限个: $P_1, P_2, \cdots, P_k$, 于是我们有两个目标, 一是构造一个自然数N 它具有素因子P 且$P\neq P_i(1\leq i\leq k)$, 二是P 具有$4n-1$形式, 为保证目标一的实现只须令$N=a(P_1\cdot P_2\cdots P_k)^m+b$其中$a, b\in Z-\{0\}$, $m\in N$, $P|N$, $P|b$。这是因为若P 与某一个$P_i(1\leq i\leq k)$相同, 则$P|a(P_1\cdot P_2\cdots P_k)^m$, 从而$P|N-a(P_1\cdot P_2\cdots P_k)^m$即$P|b$这与$P|b$矛盾。为达到目标二, 考虑到奇素数只有两类: $4n-1, 4n+1(n\in N)$, 所以只须保证N 的素因子不全是$4n+1$类型即可。为此可令$N=a(P_1\cdots P_k)^m+b$, 其中m 为偶数, $a+b\not\equiv1(mod4)$。这是因为若N 的素因子全是$4n+1$形式必有$N\equiv1(mod4)$, 但$N\equiv a+b(mod4)$故$N\not\equiv1(mod4)$, 由上面分析易见a、b 取法很多, 这给我们解决问题带来很大的游刃空间。

证明　令$N=4(P_1\cdot P_2\cdots P_k)^2-1$, 易见$N>1$且N 是奇数。设P 是N 的素因子, 则由前面的分析知:

(1)　P 与P_i互异$(1\leq i\leq k)$且$P\neq2$;

(2)　$N\equiv3(mod4)$, 故N 必有一个素因子P 是有$4n-1$形式, 这与假设矛盾, 从而形如$4n-1(n\in N)$形式的素数具有无穷多个。

命题2　形如$4n+1(N\in N)$形式的素数具有无穷多个。

[分析]反设具有$4n+1$形式的素数只有有限个: $P_1, P_2, \cdots, P_k$。从命题1的分析可以看到目标一是较易于实现的, 关键在于目标二。设P 是N 的奇素因子则, $N\equiv O(modp)$, 由二次剩余及欧拉判别法则推论知为保证N 一定具有模4为1的素因子P, 只须$N-1$是平方数即可。事实上, 令$N-1=X^2$则$X^2\equiv-1(modp)$, 所以$\left(\frac{-1}{P}\right)=1$, 于是必有$P\equiv1(mod4)$, 此时N 的素因子全是模4为1的。

证明　令$N=4(P_1\cdot P_2\cdot\cdots P_k)^2+1$, 于是$N>1$且N 为奇数。设P 是N 的某一素因子, 必$P\neq2$且

(1)　$P\equiv1(mod4)$;

(2)　P 异于$P_1, P_2, \cdots P_k$。

2　形如$8n+k(n\in N, k=1, 3, 5, 7)$形式素数的无穷性。

命题3　形如$8n+1(n\in N)$形式的素数有无穷多个。

引理1　设F_n是费马数(Femat), 即$F_n=2^{2^n}+1\quad(n\in Z_+)$则

(1)　如果$m>n$, 有$F_n|F_m-2$; $(m\in Z_+)$

(2)　若$m\neq n$, 则$(F_n, F_m)=1$;

(3)　若P_1, P_2是素数且$P_1|F_m, P_2|F_n$, 则$(P_1, P_2)=1$。

证明　(1)令$m=n+k(k\in N)$, $\because F_m=2^m+1$, $F_n=2^{2^n}+1$。

[收稿日期]　2002-10-10
[作者简介]　潘杨友, 池州师专数学系教师。

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$\therefore F_m - 2 = 2^m - 1 = 2^{2^{n+k}} - 1$

$= (2^{2^{n+k-1}} + 1)(2^{2^{n+k-1}} - 1)$

$= \prod_{i=1}^{k-1}(2^{2^{n+k-i}} - 1)(2^{2^n} + 1)(2^{2^n} - 1)$,

故 $F_n \mid F_m - 2$。

(2) 不妨设 $m > n$, 记 $d = (F_m, F_n)$, 由(1)知 $F_n \mid F_m - 2$, 设 $F_m - 2 = kF_n (k \in N)$, 于是 $F_m - kF_n = 2$, 又 $d \mid F_n$, 所以 $d \mid F_m - kF_n$, 即 $d \mid 2$, 故 $d = 1$ 或 2。但 F_n, F_m 为奇数, 因此 d 只能为 1, 从而 $(F_m, F_n) = 1$。

(3) $\because (P_1, P_2) \mid (F_m, F_n)$, 而 $(F_m, F_n) = 1$, $\therefore (P_1, P_2) = 1$。

引理 2 设 P 是素数, 如果 $P \mid F_n$, 则 $P \equiv 1 (\mathrm{mod}\, 2^{n+1})$, 特别地当 $n \geq 2$ 时, F_n 的所有素因子模 8 为 1。

证明 $\because 2^{2^n} + 1 \equiv 0 (\mathrm{mod}\, p)$,

$\therefore 2^{2^n} \equiv -1 (\mathrm{mod}\, p)$ ①

由于 $(P, 2) = 1$, 故 2 关于模 P 有阶, 设其阶为 d, 于是 $2^d \equiv 1 (\mathrm{mod}\, p)$。

由①知 $2^{2^{n+1}} \equiv 1 (\mathrm{mod}\, p)$, $\therefore d \mid 2^{n+1}$ (阶的性质) 所以 $d = 2^l$ 其中 $1 \leq l \leq n+1$, 特别地 $2^2 \equiv 1 (\mathrm{mod}\, p)$, 下证 $l = n+1$。 ②

若不然 $l \leq n$, 由②两边平方可得 $2^{2^{l+1}} \equiv 1 (\mathrm{mod}\, p)$, 再两边平方有 $2^{2^{l+1}} \equiv (\mathrm{mod}\, p)$, 如此下去必可得 $2^{2^n} \equiv 1 (\mathrm{mod}\, p)$, 这与①相矛盾, 故 $d = 2^{n+1}$。

另一方面 $2^{p-1} \equiv 1 (\mathrm{mod}\, p)$ (费马定理), 从而 $d \mid (P-1)$ (阶的性质), 所以 $2^{n+1} \mid P-1$, 即 $P \equiv 1 (\mathrm{mod}\, 2^{n+1})$。

命题 3 的证明:

反设具有 $8n+1$ 形式的素数仅有 k 个, 由于素数具有无穷多个, 故可取 $k+1$ 个互异素数: $m_1, m_2, \cdots\cdots, m_{k+1}$。令 P_i 是 F_{m_i} 的素因子 $(1 \leq i \leq m+1)$, 由引理 2 可得 $k+1$ 个具有 $8n+1$ 形式的素数 $P_1, P_2, \cdots\cdots, P_{k+1}$。由于 $(m_i, m_j) = 1 (1 \leq i \neq j \leq k+1)$。所以 $(F_{m_i}, F_{m_j}) = 1$, 由引理 1 必有 $P_1, P_2, \cdots, P_{k+1}$ 互异, 于是我们就得到了 $k+1$ 个具有 $8n+1$ 形式的互异素数, 这与已知反设矛盾。

命题 4 形如 $8n+3 (n \in N)$ 形式的素数有无穷多个。

证明 令 $N = (P_1 \cdot P_2 \cdot \cdots P_k)^2 + 2$, 则 N 是奇数。设 P 是 N 的素因子, 则 $P \neq 2$ 且

(1) P 与 P_i 互异的 $(i = 1, 2, \cdots, k)$;

(2) $P \equiv 1 (\mathrm{mod}\, 8)$ 或 $(P \equiv 3 (\mathrm{mod}\, 8)$。

这是因为 $(\frac{-2}{P}) = 1$, 所以 $(\frac{2}{P})(\frac{-1}{P}) = 1$。

当 $(\frac{2}{P}) = 1$, $(\frac{-1}{P}) = 1$ 时

由欧拉(Euler)判别法的推论知 $P \equiv 1 (\mathrm{mod}\, 8)$

当 $(\frac{2}{P}) = -1$, $(\frac{-1}{P}) = -1$ 时, 由欧拉判别法的推论知 $P \equiv 3 (\mathrm{mod}\, 8)$。

(3) N 的素因子不可能全是模 8 为 1。

考虑到若干个模 8 为 1 的素数之积仍是模 8 为 1, 但 $N \neq 1 (\mathrm{mod}\, 8)$, 这是因为 $P_i^2 \equiv 1 (\mathrm{mod}\, 8) (i = 1, 2, \cdots, k)$, 所以 $(P_1 \cdot P_2 \cdots P_k)^2 \equiv 1 (\mathrm{mod}\, 8)$, 故 $N \equiv 3 (\mathrm{mod}\, 8)$, 由(2)(3)可见 N 必具有模 8 为 3 的素因子 P。

命题 5 形如 $8n+5 (n \in N)$ 形式的素数有无穷多个。

[分析]由于模 4 为 1 的数仅有两类, 一类是模 8 为 5, 另一类是模 8 为 1。从命题 2 的分析可知, 我们可以构造一个奇自然数 N, 它的全部素因子仅具有模 4 为 1 的形式, 为保证 N 一定具有模 8 为 5 的素因子, 只须 $N \neq 1 (\mathrm{mod}\, 8)$ 这是因为模 8 为 1 的因子之积仍是模 8 为 1 的。

证明 : 反设形如 $8n+5 (n \in N)$ 形式的素数仅有有限个: $P_1, P_2, \cdots\cdots, P_k$, 令 $N = 4(P_1 \cdot P_2 \cdots P_k)^2 + 1$, 并设 P 是其素因子, 于是我们有

① $P \mid (2P_1 \cdot P_2 \cdots P_k)^2 + 1$, 从而 $(\frac{-1}{P}) = 1$, 所以 $P \equiv 1 (\mathrm{mod}\, 4)$, 即 N 的素因子全是模 4 为 1 的。

(2) P 与 $P_i (1 \leq i \leq k)$ 互异。

(3) N 一定具有形如 $8n+5$ 形式的素因子 P。

$\because P_i \equiv 5 (\mathrm{mod}\, 8)$, $\therefore P_i^2 \equiv (\mathrm{mod}\, 8) (1 \leq i \leq k)$, 从而 $4(P_1 \cdots P_k)^2 \equiv 4 (\mathrm{mod}\, 8)$, 故 $N \equiv 5 (\mathrm{mod}\, 8)$, 这时 $N \neq 1 (\mathrm{mod}\, 8)$。

命题 6 形如 $8n+7 (n \in Z_+)$ [即 $8n-1 (n \in N)$]形式的素数有无穷多个。

证明 令 $N = (P_1 \cdot P_2 \cdots P_k)^2 - 2$, 设 P 是其素因子, 则 $N \equiv 0 (\mathrm{mod}\, p)$, 即 $(P_1 \cdot P_2 \cdots P_k)^2 - 2 \equiv 0 (\mathrm{mod}\, p)$, 故 $(\frac{2}{P}) = 1$, 由欧拉判别法推论知 $P \equiv \pm 1 (\mathrm{mod}\, 8)$, 也就是说 N 的素因子不是模 8 为 1 的就是模 8 为 -1 的。

往证 N 一定具有 $8n-1$ 形式的素因子 P。

事实上, $\because P_i \equiv -1 (\mathrm{mod}\, 8)$, $\therefore P_i^2 \equiv 1 (\mathrm{mod}\, 8) (1 \leq i \leq k)$ 故 $N \equiv -1 (\mathrm{mod}\, 8)$, 由此可见 N 的素因子不可能全是模 8 为 1 的又 $P \mid 2$, 易见 P 与 $P_i (1 \leq i \leq k)$ 互异, 这样我们就又得到了具有 $8n-1$ 形式的新素数 P, 从而与假设矛盾。

3 有限群特征标与狄利克雷定理

3.1 狄利克雷(Dirichlet)定理

若 $K, L \in N$, $(K, L) = 1$ 则形如 $Kn+L$ 形式的

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

素数的个数无穷。

数论与群论有着相辅相成与密不可分的关系——数论为群论提供了直观的背景，对群论中若干概念的涵义和相互关系提供了易于理解的具体模型与形象，而群论特别是有限群理论又为数论的研究提供了形式工具和简明有效的证明方法，鉴于此本文想利用有限群的特征标概念与性质来解释狄利克雷定理。

3.2 有限群特征标及性质

设 G 是一个有限群，G 到复数域 C 上的一个表示 f: G→GL (n, C) 是同态映射，其中 GL (n, c) 是 C 上的 n×n 阶非奇异矩阵所形成的乘法群。

例如 5 元交代群 A_5 是一个阶为最小的非交换单群，$|A_5| = 60$，如果把群 A_5 看作 C 上五维向量空间 V 的基底 $\{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5\}$ 的置换，我们就可以将 A_5 的每一个元素同一个 5×5 阶矩阵联系起来。

如果 G 的两个同态表示 f_1、f_2 满足：存在矩阵 A ($|A| \neq 0$)，使得对任意的 $g \in G$，恒有 $f_1(g) = A^{-1} f_2(g) A$，则称 f_1 与 f_2 是等价的。

设 f 是 G 的一个同态表示，它满足

$$f'(g) = \begin{pmatrix} f_1(g) A_{1,n-1} \\ 0 & f_2(g) \end{pmatrix}, \quad ①$$

其中 $f_1(g)$、$f_2(g)$ 分别表示 1×1 阶和 $(n-1)\times(n-1)$ 阶矩阵，$(n \geq 2, n \in N)$，如果 G 的表示 f 不与 f 等价，则称 f 是 G 的不可约表示。

从 G 到 C 中映射△: $g \to Trace(f(g))$ 称为 f 的特征标。表示的特征标△是 G 上的类函数，即 $\triangle(a^{-1}ga) = \triangle(g)$，对所有 $g \in G$，且对任何特征标△有 $\triangle(g_1 g_2) = \triangle(g_1)\triangle(g_2)$，对任意的 $g_1, g_2 \in G$ 等价表示有相同的特征标。形如 $a^{-1}ga$ 的全体元素的集合是群 G 的共轭类。其中 g 是一定元，a 跑遍群 G。

我们已经知道，G 的不可约表示等价类的数目正好等于 G 的共轭类的类目。若设 G 的相异不可约特征标为 $\triangle_1, \triangle_2, \cdots, \triangle_r$（这里 r 是 G 的共轭类数目），我们就可以得到一个 r×r 阶正方表。它给出这些特征标在 G 的共轭类的代表元上的值，此表称为 G 的特征标表。它能决定 G 是单群或是可解群，还能定出其子群。查看此表还能决定一个元素是否为换位子，即形如 $x^{-1}y^{-1}xy$ 的元素（其中 $x, y \in G$）。

群的特征标 $\triangle_1, \triangle_2, \cdots \triangle_r$ 满足正交关系：

$$\frac{1}{|G|}\sum_{g \in G} \triangle_i(g)\overline{\triangle_j(g)} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

$$\sum_{i=1}^{r} \triangle_i(g)\overline{\triangle_j(n)} = \begin{cases} |G| / |\varphi(g)| & \text{若 } g, n \text{ 属于同一共轭类 } \varphi(g), \\ 0 & \text{其它情况。} \end{cases} \quad ②$$

3.3 Dirichlet 定理的证明

先引入狄利克雷的 L——函数 L (S, △)：

令 $\triangle_k^*$ 表示单位元群，即整数模 k 所得同余类环 $\triangle_k$ 中所有可逆元对乘法所作的群。Z 是这个群的特征标，利用下式将 Z 升为 Z 上的函数

$$\triangle(n) = \begin{cases} \triangle(\bar{n}), & \text{若 } (n, m) = 1 \\ 0, & \text{其它} \end{cases} \quad ③$$

这里 $\bar{n}$ 是在典范映射 $Z \to Z_k$ 之下的象。

定义 L (S, △) 为：

$$\log L(S, \triangle) = \sum_P \sum_{m=1}^{\infty} \frac{\triangle(P^m)}{m P^{ms}} = \sum_P \frac{\triangle(P)}{P^s} + \sum_{m=2}^{\infty} \frac{(P^m)}{m P^{ms}}, Re(s) > 1 \quad ④$$

现取△为 $\triangle_k^*$ 的不可约特征标，按③的办法将△升为△上互数，选取 $t \in Z$，使得 $tL \equiv 1 (\mathrm{mod}\, k)$，再用 $\triangle(t)$ 乘以④，并对 Z_k^* 的所有不可约特征求和可得：

$$\sum_{\triangle} \triangle(t) \log L(S, \triangle) = \sum_P \sum_{\triangle} \triangle(P) P^{-s} + \sum_{\triangle} \sum_{m=2}^{\infty} \frac{\triangle(t)\triangle(P^m)}{m P^{ms}} \quad ⑤$$

由①知 $\triangle(t)\triangle(P) = \triangle(tp)$，用②取其中一个元素为 1，就可得

$$\sum_{Z} \triangle(tp) = \begin{cases} |\triangle_k^*| & \text{若 } tp \equiv 1 (\mathrm{mod}\, k) \\ 0 & \text{若 } tp \not\equiv 1 (\mathrm{mod}\, k) \end{cases}$$

而 $tL \equiv 1 (\mathrm{mod}\, k)$，$tp \equiv 1 (\mathrm{mod}\, p)$ 等价于 $P \equiv L (\mathrm{mod}\, k)$，因而⑤式右边第一项化为 $|\triangle_k^*| \sum_{P \equiv L (\mathrm{mod}\, k)} P^{-s}$。

可以证明，当 S 沿着实轴超于 1^+ 时，⑤式左边趋于∞，而右边第二项超于有限极限值，故得 $\sum_{P \equiv L (\mathrm{mod}\, k)} P^{-s}$ 发散，从而证明了定理。

[参　考　文　献]

[1] 冯克勤，余红兵 整数与多项式[M]，北京：高等教育出版社，海德堡施普林格出版社，1999.

[2] 闵嗣鹤，严士健 初等数论[M]，北京：高等教育出版社，1998.

[3] 中国科学院数学研究所，数学译林，第二卷，第 1 期，1983.

[4] K. chandrsekharan, Introduction to Analytic Number Theory[M], Springer-Verlag, 1968.

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net